นโยบายระบบบริหารจัดการความปลอดภัยสารสนเทศ

Information Security Management System Policy

TOG manufactures spectacle lenses, supplying business customers, both domestically and internationally. We pay close attention to the security of all data, as well as all information systems, according to the Principles of Confidentiality, Integrity and Availability (CIA), to continuously develop the organization of information and protect data, in a quality manner, and to manage data as an asset for driving business. Reviewed at least once a year, the following outlines the Information Security.

1.Establish an Information Security Management System (ISMS) in accordance with ISO/IEC 27001 and be certified by the relevant certification bodies.

2. Adopt security controls and techniques to manage information security, using the ISO/IEC 27002, risk management principles, and applicable legal requirements as guidelines, to establish appropriate, relevant practices, and provide training and awareness programs to foster a strong security culture

3.The management, employees and all involved parties shall recognize the importance of, understand its requirements, actively participate in the management of the Information Security Management Systems, according to ISO/IEC 27001 standard, and continuously pursue improvement.

4.The management, employees and all involved parties have a duty and responsibility to continuously control, evaluate and review Information Security Management, to ensure that important information and personal data is private, accurate and updated, at all times, and that appropriate mechanisms are in place, to uninterruptedly control the management of information systems. along with ensuring the systematic and reliable management of security incidents.

นโยบายระบบบริหารจัดการความปลอดภัยสารสนเทศ

TOG ผลิตเลนส์สายตาซัพพลายลูกค้าธุรกิจทั้งในประเทศและต่างประเทศ เราให้ความสำคัญต่อการรักษาความมั่นคงปลอดภัยของข้อมูลที่สำคัญ ตลอดจนระบบสารสนเทศ ตามหลักการ CIA ปกป้องความลับ (Confidentiality) ถูกต้องแม่นยำ เป็นปัจจุบัน (Integrity) และ พร้อมใช้งาน (Availability) เพื่อพัฒนาความสามารถในการจัดการข้อมูลและปกป้องข้อมูลอย่างมีคุณภาพ ใช้ข้อมูลให้เป็นสินทรัพย์อย่างหนึ่งในการขับเคลื่อนธุรกิจ จึงทบทวนอย่างน้อยปีละ 1 ครั้ง และกำหนดนโยบายระบบบริหารจัดการความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ดังนี้

1.จัดทำระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) ตามมาตรฐาน ISO/IEC 27001 และได้รับการรับรองจากหน่วยงานที่ให้การรับรอง

2.นำการควบคุมและเทคนิคความปลอดภัย มาใช้ในการจัดการความปลอดภัยด้านสารสนเทศ โดยใช้ ISO/IEC 27002 หลักการจัดการความเสี่ยง และข้อกำหนดทางกฎหมายที่เกี่ยวข้องเป็นแนวทาง เพื่อสร้างแนวปฏิบัติที่เกี่ยวข้องอย่างเหมาะสม และจัดโปรแกรมฝึกอบรมและการสร้างความตระหนักรู้เพื่อส่งเสริมวัฒนธรรมความปลอดภัยที่เข้มแข็ง

3.ผู้บริหาร พนักงาน และบุคคลากรที่เกี่ยวข้องตระหนักถึงความสำคัญ เข้าใจข้อกำหนดต่างๆ มีส่วนร่วมอย่างแข็งขันในการจัดการระบบการจัดการความปลอดภัยสารสนเทศ ตามมาตรฐาน ISO/IEC 27001 และ ดำเนินการปรับปรุงอย่างต่อเนื่อง

4.ผู้บริหาร พนักงาน และบุคคลากรที่เกี่ยวข้อง มีหน้าที่ ควบคุม ประเมินผล ทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง เพื่อให้แน่ใจว่าข้อมูลสำคัญและข้อมูลส่วนบุคคลมีความปลอดภัย ถูกต้องแม่นยำ เป็นปัจจุบัน และมีกลไกควบคุมการจัดการระบบข้อมูลให้พร้อมใช้งานอยู่เสมอ พร้อมทั้งสามารถจัดการกับเหตุการณ์ด้านความมั่นคงปลอดภัยได้อย่างเป็นระบบและเชื่อถือได้

TOG
THAI OPTICAL GROUP